

Resolved, That the Senate Legal Counsel is authorized to represent Secretary Thomson and Mr. Wineman in the case of *Newdow v. Eagen*, et al.

AUTHORIZING REPRESENTATION BY SENATE LEGAL COUNSEL

Mr. REID. Mr. President, I ask unanimous consent the Senate proceed to S. Res. 344.

The PRESIDING OFFICER. The clerk will report the resolution by title.

The legislative clerk read as follows:

A resolution (S. Res. 344) to authorize representation by the Senate Legal Counsel in *Manshardt v. Federal Judicial Qualifications Committee*, et al.

There being no objection, the Senate proceeded to consider the resolution.

Mr. DASCHLE. Mr. President, an unsuccessful applicant for U.S. Attorney in Los Angeles has commenced a civil action in Federal court in California against Senator FEINSTEIN, Senator BOXER, a prominent Republican businessman and political leader in California, and a judicial screening panel set up by these defendants, to challenge the use of this screening panel to identify potential nominees for Federal District Court judgeships in California. Specifically, the plaintiff alleges that the use of informal screening panels to develop lists of potential judicial nominees violates the Federal Advisory Committee Act, the Government in the Sunshine Act, and the separation of powers.

The laws underlying this suite do not apply to the Senate, and the Speech or Debate Clause bars suits against legislators for the performance of their duties under the Constitution. Thus, there is no legal basis for suing Senators for their role in forming, appointing, or relying on judicial screening panels.

Further, the use of informal judicial selection panels to identify potential judicial nominees as a part of the advice and consent function has a long and respected history. Also, the Supreme Court's holding in *Public Citizen versus U.S. Department of Justice* that the Federal Advisory Committee Act does not apply to the longstanding practice of soliciting views on prospective judicial nominees from an American Bar Association committee provides ample support for the challenged practice.

This resolution would authorize the Senate legal counsel to represent the Senators sued in this action to protect their role in the advice and consent process by which the President and the Senate share responsibility for the appointment of Federal judges under the Constitution.

Mr. REID. Mr. President, I ask unanimous consent the resolution and preamble be agreed to, the motion to reconsider be laid on the table, and that any statements in relation thereto be printed in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The resolution (S. Res. 344) was agreed to.

The preamble was agreed to.

The resolution, with its preamble, reads as follows:

S. RES. 344

Whereas, Senators Dianne Feinstein and Barbara Boxer have been named as defendants in the case of *Manshardt v. Federal Judicial Qualifications Committee*, et al., Case No. 02-4484 AHM, now pending in the United States District Court for the Central District of California; and

Whereas, pursuant to sections 703(a) and 704(a)(1) of the Ethics in Government Act of 1978, 2 U.S.C. §§288b(a) and 288c(a)(1), the Senate may direct its counsel to represent Members of the Senate in civil actions with respect to their official responsibilities: Now, therefore, be it

Resolved, That the Senate Legal Counsel is authorized to represent Senators Dianne Feinstein and Barbara Boxer in the case of *Manshardt v. Federal Judicial Qualifications Committee*, et al.

CYBER SECURITY RESEARCH AND DEVELOPMENT ACT

Mr. REID. Mr. President, I ask unanimous consent the Senate now proceed to Calendar No. 549, S. 2182.

The PRESIDING OFFICER. The clerk will report the bill by title.

The legislative clerk read as follows:

A bill (S. 2182) to authorize funding for the computer and network security research and development and research fellowship programs, and for other purposes.

There being no objection, the Senate proceeded to consider the bill.

CHECKLIST PROVISION—CYBER SECURITY RESEARCH AND DEVELOPMENT ACT, HR 3394

Mr. HOLLINGS. I would like to engage in a brief colloquy with the ranking member of the Science, Technology, and Space Subcommittee of the Commerce Committee, Senator ALLEN, regarding the provisions of H.R. 3394 that provide for the National Institute of Standards and Technology, NIST, to develop checklists for widely used software products.

Mr. ALLEN. The committee, particularly Senators WYDEN and EDWARDS, working with NIST and industry, have reached agreement on this provision. We recognize that there is no "one-size-fits-all" configuration for any hardware or software systems. We have given NIST flexibility in choosing which checklists to develop and update. We have not required any Federal agency to use the specific settings and options recommended by these checklists.

Mr. HOLLINGS. The ranking member is correct. Our intent with this provision is not to develop separate checklists for every possible Federal configuration. Rather, the checklists would provide agencies with recommendations that will improve the quality and security of the settings and options they select. The use of any checklist should, of course, be consistent with guidance from the Office of Management and Budget.

Mr. ALLEN. I agree with the chairman.

Mr. WYDEN. Mr. President, I would like to say a few words about the Senate's passage of the Cybersecurity Research and Development Act.

Americans today live in an increasingly networked world. The spread of the Internet creates lots of great new opportunities. But there is also a downside: security risks. The Internet connects people not just to friends, potential customers, and useful sources of information, but also to would-be hackers, viruses, and cybercriminals.

In July 2001, after I became chairman of the Science and Technology Subcommittee of the Senate Commerce Committee, I chose cybersecurity as the topic for my first hearing. The message from that hearing was that cybersecurity risks are mounting. And that was before the horrific attacks of September 11 hammered home the point that there are determined, organized enemies of this country who wish to wreak as much havoc as they can. The terrorists are looking for vulnerabilities, and they are not technological simpletons.

This legislation is essential to the Nation's effort to address cybersecurity threats. It is a necessary complement to both the homeland security legislation pending in Congress and to the draft cybersecurity strategy released on September 18 by the administration. Because reorganizing the Federal Government to deal more effectively with security threats is only part of the battle. The same goes for many of the steps called for in the Administration's cybersecurity strategy.

In the long run, all Government and private sector cybersecurity efforts depend on people—trained experts with the knowledge and skills to develop innovative solutions and respond creatively and proactively to evolving threats. Without a strong core of cybersecurity experts, no amount of good intentions and no amount of Government reorganizing will be sufficient to keep this country one step ahead of hackers and cyberterrorists.

Therefore, this legislation makes a strong commitment to support basic cybersecurity research, so that the country's pool of top-flight cybersecurity experts can keep pace with the evolving risks. Specifically, the bill authorizes \$978 million over five years to create new cybersecurity research and development programs at the National Science Foundation, NSF, and the National Institute of Standards and Technology, NIST. The NSF program will provide funding for innovative research, multidisciplinary academic centers devoted to cybersecurity, and new courses and fellowships to educate the cybersecurity experts of the future. The NIST program likewise will support cutting-edge cybersecurity research, with a special emphasis on promoting cooperative efforts between government, industry, and academia.

All of these programs will support advanced cybersecurity research at a